Network Security

Department	Information technology
Faculty	Computer Science
Course Code	CS.IT.0743
Course Title	Network Security
Credits	3
Pre-Requisite	Network Security
Course Instructor	Ahmad Fahiz Noori
Text Book	Network security and Network Attacks" by William stalling 6th edition.
Reference Book	Network Security and System security" by John A UACCA

1. Course Description:

The ability to secure information within a modern enterprise—large or small—is a growing challenge. Threats to information security are global, persistent, and increasingly sophisticated. Long gone are the days when managers could hope to secure the enterprise through ad hoc means.

Effective information security at the enterprise level requires participation, planning, and practice. It is an ongoing effort that requires management and staff to work together from the same script. Fortunately, the information security community has developed a variety of resources, methods, and best practices to help modern enterprises address the challenge.

Unfortunately, employing these tools demands a high degree of commitment, understanding, and skill—attributes that must be sustained through constant awareness and training.

It is important to note as well that effective security is not achieved in stovepipes. Ineffective physical security, for example, can undermine otherwise effective information system security, and vice versa. Effective security at the enterprise level requires the effective interaction of physical security, information security, personnel security, and so on—indeed, all branches of security must interact effectively as a system to achieve overall enterprise security.

2. Course Learning Outcome (CLO):

At the end of the course the Students should be able to:

1. Assess the current security landscape, including the nature of the threat, the general status of common vulnerabilities, and the likely consequences of security failures;

2. Critique and assess the strengths and weaknesses of general Network security models, including the CIA triad; Appraise the interrelationships among elements that comprise a modern security system, including hardware, software, policies, and people;
3. Assess how all domains of security interact to achieve effective system-wide security at the enterprise level.
4. Compare the interrelationships among security roles and responsibilities in a modern information-driven enterprise —to include interrelationships across security domains (IT, physical, classification, personnel, and so on);
5. Assess the role of strategy and policy in determining the success of information security;
6. Estimate the possible consequences of misaligning enterprise strategy, security policy, and security plans;
7. Design a notional information security plan that incorporates relevant principles of lifecycle management;
8. Evaluate the principles of risk and conduct a notional risk management exercise;
9. Assess the role of good metrics and key performance indicators (KPIs) in security assessment and governance;
10. Create a good set of information security metrics;
11. Critique the current legal and regulatory environment as it applies to Network security;
12. Identify and contrast the most common security standards and associated catalogues of security controls;
13. Contrast the various approaches to security training and formulate a simple training

Learning Domain:

- Cognitive (knowledge)
- Affective (Attitude)
- Psychomotor (Physical or Manual skills)

Only cognitive domain is used for this course while the rest two cannot applied here

3. Course Learning Objectives Mapping with Bloom Taxonomy:

1. Remembering
2. Understanding
3. Applying
4. Analyzing

5. Evaluating
6. Creating

COLs	1	2	3	4	5	6
1	**Yes**	**Yes**				
2		**Yes**	**Yes**			
3			**Yes**	Yes		
4		**Yes**		**Yes**		**Yes**

1. Course Teaching Methods

1	Lecture
2	Problem solving Learning
3	Interactive Learning
4	Practical Examples

2. Grading Scheme

Mid Term	20%
Assignment	10%
Quiz	10%
Final Term	60%

3. Weekly Course Breakdown:

Week	Topic	Learning Outcome	Instructor Activities	Student Activities	Assessment
1	The Security Environment • Threats, vulnerabilities, and consequences • Advanced persistent threats • The state of security today • Why security matters to DoD	At the end of the lecture the students will be able to: understand about security and security attack categories.	• Lecture presentation • Summarizing the lecture	• Group discussion as class activity. • Brain Storming	Question from students regarding network security
2	Principles of Network security • The interrelated components of the computing	At the end of the lecture the students will be able to: Know about CIA triangle,	• Asking the students about the topic • Lecture	• Group discussion as class activity. • Brain	Asking questions about CIA triangle and Exploiters Assignment

	environment • Network security models (the CIA triad, the star model, the Parkerian hexad) • Variations on a theme: computer security, information security, and information assurance	security needs and Exploiters	presentation • Summarizing the lecture	Stormin g	
3	Network security Management Concepts • Security governance • Management models, roles, and functions	At the end of the lecture the students will be able to: Understand threat modeling and Risk assessment	• Asking the students about the previous topic. • Lecture presentation • Summarizing the lecture	• Group discussi on as class activity. • Note taking • Brain Stormin g	Asking questions from the students about Threat Modeling and risk assessment Assignment
4	Enterprise Roles and Structures • Information security roles and positions Alternative enterprise structures and interfaces	At the end of the lecture the students will be able to: Know about security aspects and how to get secure, security mechanism.	• Asking the students about the previous topic. • Lecture presentation • Summarizing the lecture	• Group discussi on as class activity. • Note taking • Brain Stormin g	Asking questions from the students about: 3 aspects of security and security mechanism

5	Strategy and Strategic Planning • Strategy • Strategic planning and security strategy • The information security lifecycle • Architecting the enterprise	At the end of the lecture the students will be able to: understand about the history of cryptography, basic terminology of cryptography and classification of cryptography	• Lecture presentation • Summarizing the lecture	• Group discussion as class activity. • Note taking • Brain Storming	Asking questions from the students about: History of cryptography and terminology of cryptography
6	Security Plans and Policies • Levels of planning • Planning misalignment • The System Security Plan (SSP) • Policy development and implementation	At the end of the lecture the students will be able to: Understand symmetric cryptography	• Asking the students about the previous topic. • Lecture presentation	• Group discussion as class activity. • Note taking • Brain Storming	Asking questions from the students about: Symmetric cryptography
7	Laws and Regulatory Requirements • Timeline of U.S. laws related to information security • The Federal Information Security Management Act (FISMA)	At the end of the lecture the students will be able to: know about modern symmetric cipher	• Lecture presentation • Summarizing the lecture	• Group discussion as class activity. • Note taking • Brain Storming	Asking questions from the students about: Modern symmetric cipher
8	Security Standards and Controls • Security standards and controls • Certification and accreditation (C&A)	At the end of the lecture the students will be able to: Electronic code Book	• Asking the students about the previous topic. • Lecture presentation • Summarizing the lecture	• Brain storming • Discussion • listening the lecture	Asking questions from the students about: Cipher Block chaining, modular Mathematics

					and method to encrypt messages
9	Risk Management • Principles of risk • Types of risk • Risk strategies • The Risk Management Framework (RMF)	At the end of the lecture the students will be able to: Understand RSA Public key system, Trapdoor and Deffie-Hellman Alogrithm	• Asking the students about the previous topic. • Lecture presentation • Summarizing the lecture	• Brain stormin g • Discussi on • listening the lecture	Asking questions from the students about: Public key system and related algorithms
10	Security Metrics and Key Performance Indicators (KPIs) • The challenge of security metrics • What makes a good metric • Approaches to security metrics Metrics and FISMA	At the end of the lecture the students will be able to: Understand different authentication methods	• Asking the students about the previous topic. • Lecture presentation • Summarizing the lecture	• Brain stormin g • Discussi on • listening the lecture	Asking questions from the students about: Different authenticatio n mechanism
11	Physical Security and Environmental Events • Physical and environmental threats Physical and environmental controls Introduction to IPS	At the end of the lecture the students will be able to: know about Hash Algorithm/Mess age Digest	• Lecture presentation • Summarizing the lecture	• Brain stormin g • Discussi on • listening the lecture	Asking questions from the students about: MD2 and MD4
12	Contingency Planning • Developing a contingency plan • Understanding the different types of contingency plan • Responding to events Configuring Site-to-Site VPNs	At the end of the lecture the students will be able to: understand Digital Signature, trusted intermediaries and key distribution protocol	• Asking the students about the previous topic. • Lecture presentation Summarizing the lecture	• Brain stormin g • Discussi on • listening the lecture	Asking questions from the students about: Digital signature and key distribution protocol
13	Security	At the end of	• Asking the	• Brain	Asking

	Education, Training, and Awareness • Human factors in security • Developing and implementing a security training plan Cross-domain training (IT and other security domains)	the lecture the students will be able to: Understand Digital certificate	students about the previous topic. • Lecture presentation • Summarizing the lecture	stormin g • Discussi on • listening the lecture	questions from the students about: Digital certificate Assignment
14	Managing information security across the DoD enterprise (1) • The purpose of certification and accreditation • Trends in certification and accreditatio n	At the end of the lecture the students will be able to: understand Email and Email architecture	• Asking the students about the previous topic. • Lecture presentation • Summarizing the lecture	• Brain stormin g • Discussi on • Note taking	Asking questions from the students about: PGP Threats
15	Managing information security across the DoD enterprise (2) • The strategic direction of DoD IT and information security • Responsibilities within the DoD enterprise	At the end of the lecture the students will be able to: understand IPsec and firewalls	• Asking the students about the previous topic. • Lecture presentation • Summarizing the lecture	• Brain stormin g • Discussi on • Note taking	Asking questions from the students about: IPsec Firewalls
16	The future of Network security • Key future uncertainties • Possible future scenarios How to apply what you've learned	At the end of the lecture the students will be able to: understand packet filter, application level gateway, hybrid, privacy enhance mail (PEM), structure of	• Asking the students about the previous topic. • Lecture p.resentation	• Brain stormin g • Discussi on • Note taking	Asking questions from the students about: Packet filter Structure of PEM Quiz

		PEM and source authentication and integrity protection			

References:

Stalling, W. (2018). *Cryptography and Network security 6th edition.* Pearson.

UACCA, J. A. (2016). *Network Security and Network Attacks.* Syngress